(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 505 780 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
23.03.2011 Bulletin 2011/12

(51) Int Cl.:
H04W 8/08 *(2009.01)*

(21) Application number: **03291964.9**

(22) Date of filing: **06.08.2003**

(54) **A method of validated communication**

Verfahren zur validierten Kommunikation

Procédé pour une communication validée

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PT RO SE SI SK TR

(43) Date of publication of application:
09.02.2005 Bulletin 2005/06

(73) Proprietor: **MOTOROLA, INC.**
Schaumburg, IL 60196 (US)

(72) Inventors:
- **Olivereau, Alexis**
  91120 Palaiseau (FR)
- **Janneteau, Christophe**
  78390 Bois D'Arcy (FR)
- **Petrescu, Alexandru**
  91400 Orsay (FR)

(74) Representative: **Cross, Rupert Edward Blount et al**
Boult Wade Tennant
Verulam Gardens
70 Gray's Inn Road
London WC1X 8BT (GB)

(56) References cited:
EP-A- 1 158 742 **WO-A-03/047183**
US-A1- 2003 095 523

- **D. JOHNSON, RICE UNIVERSITY; C. PERKINS, NOKIA RESEARCH CENTER; J. ARKKO, ERICSSON: "Mobility Support in IPv6" IETF MOBILE IP WORKING GROUP, INTERNET DRAFT, [Online] 30 June 2003 (2003-06-30), XP002267140 Retrieved from the Internet: <URL: http://www.ietf.org/ids.by.wg/mip6.ht ml> [retrieved on 2004-01-13]**

EP 1 505 780 B1

Description

Technical Field

[0001] The invention relates to a method of validated communication, in particular, it relates to a method of validated communication between a mobile network node and a correspondent node via at least a first mobile router.

Background

[0002] Traditional mobility support aims to provide continuous Internet connectivity to mobile hosts, such as for example a laptop computer with wireless connectivity. By contrast, network mobility support is concerned with situations where an entire network comprising potentially many hosts changes its point of attachment to the Internet topology and thus the route to reach it in the topology. Such a network in movement can be called a Mobile Network.

[0003] A number of scenarios exist where such Mobile Networks occur. To give just two examples:

i. A Personal Area Network (PAN, i.e. a network of several personal devices attached to an individual) will change its point of attachment to the Internet topology whilst the user is walking around town.
ii. A network embedded in a bus or aircraft providing on-board Internet access to passengers. These passengers may be using a single device (e.g. a laptop) or in turn own a Mobile Network (such as a PAN), which then illustrates the case of a Mobile Network visiting a Mobile Network (i.e. nested mobility).

[0004] A Mobile Network (MONET) can therefore be defined as a set of nodes, part of one or more IP-subnets attached to a Mobile Router (MR), that are mobile as a unit, with respect to the rest of the Internet. In other words, an MR and all its attached nodes (so called Mobile Network Nodes or MNNs).

[0005] An MNN itself may be a local fixed node (LFN) permanently associated with a given mobile network, a local mobile node (LMN) capable of altering its point of network attachment within the current mobile network and of leaving the current mobile network to attach elsewhere, or a visiting mobile node (VMN), whose home link is not on the current mobile network and has changed its point of attachment from somewhere outside the current mobile network. As noted above, the MNN can be a simple mobile host or another mobile router, resulting in nested mobility.

[0006] With the change of attachment points available to mobile networks, a method of optimising the route by which packets of data are sent and received by such networks is highly desirable for a number of reasons:

i. Route optimisation reduces delay by reducing packet path length;
ii. It increases overall available bandwidth in the system because packets are routed through a shorter path, and are no longer tunnelled;
iii. It can increase the maximum transmission unit size on the communication path, reducing fragmentation of the payload.

[0007] The Mobility Support in the IPv6 ('mobile IPv6' or MIPv6) specification (see http://www.ietf.org/) proposes means to enable Route Optimisation (bi-directional communication using the shortest path) between an MN and a correspondent node (CN), but no mechanism has been proposed as yet to enable route optimisation between an MNN and a CN.

[0008] Referring to Figure 1, the basic network mobility support ("NEMO Basic Support Protocol" at http://www.ietf.org/) for communication between an MNN and a CN relies on bi-directional tunnelling between the mobile router (MR) and its home agent (HA):

i. Inbound packets (from a CN to a MNN) are sent to the MR's home link; The MR's HA intercepts and tunnels them to the MR.
ii. Outbound packets (from an MNN to a CN) are reverse-tunnelled by the MR to its HA.

[0009] However, this does not provide route optimisation to the MNN.

[0010] EP 1 158 742 A1 and associated paper, "Mobile Networks Support in Mobile IPv6 (Prefix Scope Binding Updates)", by T. Ernst, A. Olivereau, L. Bellier, C. Castelluccia, H. -Y. Lach, IETF Internet-Draft draft-ernst-mobileip-v6-network-03.txt, March 2002, describe how when an MR roams to a visited network, it sends a modified version of the MIPv6 binding update (BU), referred to by these documents as a prefix scope binding update (PSBU), to its home agent (HA).

[0011] Likewise, the solution presented in US2003/0095523 considers a modified binding update sent by a MR to its HA.

[0012] the classical MIPv6 BU only informs the CN of where to send data addressed to a single mobile node (e.g. the mobile routers home address (HoA) coupled to a roving care-of address (CoA)). The proposed PSBU does not bind an MR HoA to an MR CoA but the MR prefix to the MR CoA, thus informing the HA receiving the PSBU to send data addressed to any MNN attached to the MR on to the MR CoA.

[0013] Upon reception of a packet whose destination address matches with the MR prefix (e.g. the destination is an MNN), the Home Agent (HA) must then tunnel the packet to the MR CoA that will deliver it to the actual recipient.

[0014] Similarly the MR may send PSBUs to the correspondent nodes of the MNNs, which would achieve CN / MNN route optimisation.

[0015] However, this solution is only acceptable if the

PSBU can be successfully validated by its recipient. Beyond peer authentication, the PSBU sender has to actually prove that it owns the whole prefix that it sends a PSBU for.

[0016] This is not a problem as long as the recipient of the PSBU is the MR Home Agent, which is expected to have initial knowledge about the prefix that belongs to the MR. However when the recipient is any CN, a mechanism has to be found to allow that CN to validate a PSBU. No mechanism has been proposed as yet, which greatly reduces the applicability of this solution.

[0017] One may consider the applicability of the methods already proposed for classic MIPv6 BU validation:

i. Cryptographically Generated Addresses.

[0018] In this solution, a home address (HoA) is bound to a public key that is part of a public/private key pair. This ensures that a malicious node cannot assume the mantle of the home address, as it does not own the corresponding private key.

[0019] In reference to PSBU, however, this method cannot be extended to prefix ownership as a large number of home addresses may share the same prefix. Moreover it is unlikely that MIPv6 or any future specification is going to allow any mobile network to assign its own address or prefix. Adding an additional hash to the prefix in order to make the ownership unique, is limited by the available number of bits in the network prefix. Estimates suggest that only 2^{16} (approximately 65,000) public keys would need to be tested by an attacker to achieve a 50% chance of losing uniqueness and thus security.

ii. Return Routability Checking Procedure (RRP).

[0020] RRPs are now incorporated within the MIPv6 specification, and consist of a check by the correspondent node (CN) to verify that the specified home address (HoA) can actually be reached at the specified care-of address (CoA), before accepting the binding update (BU). Essentially, the process comprises:

- A mobile node (MN) initiating the procedure by sending Home Test Initiation (HoTI) and Care-of Test Initiation (CoTI) messages to the CN;
- The CN sending a Home Test (HoT) message to the home address of the MN and a Care-of Test (CoT) message to the care-of address of the MN;
- From the contents of both the HoT and the CoT, The MN generates a key that it uses to sign the BU it is to send.

[0021] The MN thus needs to successfully receive both the HoT and the CoT to be able to generate a valid BU. This is considered by the CN as a sufficient proof that the home and care-of addresses are valid for that MN.

[0022] In reference to PSBU, however, this mechanism cannot be used to ensure that a whole prefix can be reached at a certain care-of address. Prefix ownership is much more than address ownership: to obtain a similar level of security, it would be necessary for the CN to check using RRP all possible addresses that can be derived from that network prefix.

[0023] This is clearly unacceptable, as standard prefix lengths lead to an enormous quantity of possible IPv6 addresses.

[0024] Consequently one concludes that PSBU cannot provide validated route optimisation to the mobile network, i.e. it cannot provide validated route optimisation to any mobile network node attached therein.

[0025] Thus a need still exists for a method of validated route optimisation for mobile network nodes.

[0026] The purpose of the present invention is to address the above need.

Summary of the Invention

[0027] The present invention provides a method of validated communication between a mobile network node (MNN) and a correspondent node (CN) via at least a first mobile router (MR) as described in the accompanying claims.

[0028] In a first aspect, the present invention provides a method of validated communication, as claimed in claim 1.

[0029] In a second aspect, the present invention provides apparatus for validated communication, as claimed in claim 32.

[0030] In a third aspect, the present invention provides a mobile router operable to perform validated communication, as claimed in claim 33.

[0031] In a fourth aspect, the present invention provides a correspondent node operable to perform validated communication, as claimed in claim 34.

[0032] Further features of the present invention are as defined in the dependent claims.

[0033] Embodiments of the present invention will now be described by way of example with reference to the accompanying drawing(s), in which:

Brief description of the drawings

[0034]

FIG. 1 is a schematic diagram of communication between a correspondent node and a mobile network node.

FIG. 2 is a comparative process chart detailing the differences between a return routability checking procedure known to the art and an extended return routability checking procedure in accordance with an embodiment of the present invention.

FIG. 3 is a block diagram of mobility options for an

extended binding update message in accordance with an embodiment of the present invention.

FIG. 4. is a schematic diagram of communication between a correspondent node and a mobile network node in accordance with an embodiment of the present invention.

FIG. 5. is a block diagram detailing successive parsing of data packets in accordance with an embodiment of the present invention.

FIG. 6. is a schematic diagram of communication between a correspondent node and a mobile network node in accordance with an embodiment of the present invention.

Detailed description

[0035] A method of validated communication is disclosed. In the following description, a number of specific details are presented in order to provide a thorough understanding of the present invention. It will be obvious, however, to a person skilled in the art that these specific details need not be employed to practice the present invention. In other instances, well known methods, procedures and components have not been described in detail in order to avoid unnecessarily obscuring the present invention.

[0036] Referring to FIG. 1, a method of validated communication is presented, between a mobile network node (MNN) 110 and a correspondent node (CN) 150 via at least a first mobile router (MR) 120.

[0037] FIG. 1 illustrates a mobile router (MR) 120 and its network that has moved from its home address 132 to an address 142 on a visited link, thus creating the need for a method of validated route optimisation for a mobile network node (MNN) (110).

[0038] Now also referring to FIG. 2, in an embodiment of the present invention, the method employs an extended return routability checking procedure (XRRP) 200, wherein an MNN test initiation (MNNTI) message is sent 236 by the MR 120, and wherein a MNN test (MNNT) message is sent 256 by the CN 150.

[0039] This adds to the security of requiring the home and care-of addresses being consistent as noted previously in standard RRPs, by enabling the generation of binding update validation keys based on receipt on any or all of the three HoT, CoT and MNNT test messages.

[0040] Additionally referring to FIG. 3, the method of this embodiment of the invention also includes sending from the MR 120 an extended binding update (XBU) 300 comprising 320 the MNN's address (MNNA) 112.

[0041] By extending the binding update to include the MNNA in this manner, validated CN / MNN route optimisation can be achieved. In particular, the validated CN / MNN route optimisation can be achieved without the need for a preestablished security context.

[0042] Additionally, it provides a suitable level of security to mobile network route optimisation - in particular a malicious node should not be able to assume the mantle of an MNN's address and redirect data elsewhere, or assume the mantle of care-of address of an MR and launch denial of service attacks on it.

[0043] Moreover, it is transparent to the MNN, so that no changes are needed to the node and consequently current equipment can enjoy the benefits of the present invention.

[0044] The extended return routability checking procedure 200 is detailed as follows:

[0045] The MR 120 detects that route optimisation is not being used for the MNN 110 whenever it receives a tunnelled packet from its home agent for that MNN 110.

[0046] Thus the validation process 200 between the MR 120 and correspondent node CN 150 is initiated upon receipt by the MR 120 of a tunnelled packet from the home agent HA 130 of the MR 120 addressed to the mobile network node MNN 110.

[0047] However, this may be subject to at least one of the following set of conditions, namely that;

i. The MNN 110 subscribes to a specified service;
ii. The CN 150 has not ignored a threshold number of prior XBUs 300;
iii. The CN 150 has not ignored a threshold number of validation processes 200; and
iv. The MNN 110 satisfies a usage policy.

[0048] Upon initiation of a validation process 200, the MR 120 generates random values (hereinafter 'cookies') for a home address test initiation (HoTI) message and a care-of address test initiation (CoTI) message, as known in the art.

[0049] In addition, however, it is now proposed that a further cookie is generated, for an additional mobile network node test initiation (MNNTI) message.

[0050] The inventors of the present invention have appreciated the need for an additional message to be employed due to the constraints of the current MIPv6 specification:

> The MR 120 is required to prove the correctness of the binding MR HoA 132 / MR CoA 142, but in addition to that proof, a third check involving the MNN 110 is necessary for the desired level of validation. Thus essentially, either the MNN 110 must be able to attest that it trusts the MR 120 to route its packets, or the MR 120 must be able to prove that it is entitled to route the packets destined to the MNN 110.

[0051] In order to retain the advantage of being transparent to the MNN 110, the inventors of the present invention chose the second mechanism: the MR 120 is to prove, upon request of the CN 150, that it is actually serving the MNN 110. MIPv6 specifies that the proof of home address ownership be performed through HoTI (Home

Test Init) and HoT (Home Test) messages respectively sent from MR HoA 132 to CN 150 and from CN 150 to MR HoA 132. Likewise, the proof of care-of address ownership is performed through CoTI (Care-of Test Init) and CoT (Care-of Test) messages respectively sent from MR CoA 142 to CN 150 and from CN 150 to MR CoA 142.

[0052] Thus the validation process (200) comprises the step (236) of the MR 120 sending a HoTI comprising the MR home address (HoA) 132 and a HoTI cookie to the CN 150; and the MR 120 sending a CoTI comprising the MR care-of address (CoA) 142 and a CoTI cookie to the CN 150 as known in the art, and additionally involves the MR 120 sending an MNNTI comprising the MNN address (MNNA) 112 and a MNNTI cookie to the CN 150.

[0053] The HoTI is sent via the MR home address (HoA) 132 and the CoTI is sent via the MR care-of address (CoA) 142.

[0054] Unlike the HoTI and CoTI messages however, the MNNTI message comprises a mobility option (as defined in MIPv6) that in turn comprises MNN address 112.

[0055] In a preferred embodiment of the present invention, the MNNTI is sent via the MR HoA 132.

[0056] In an alternative embodiment of the present invention, the MNNTI is sent via the MR care-of address (CoA) 142. The MNNTI message then additionally comprises the MR home address (HoA) 132.

[0057] In an embodiment of the present invention, upon receipt of the relevant test initiation message, the CN 150 performs the step 246 of computing a home token from an HoA 132 extracted from a HoTI, together with a random key (KCN) and a nonce (a time-dependent value), and computing a care-of token from a CoA 142 extracted from a CoTI, KCN and a nonce, as known in the art.

[0058] Additionally, upon receipt of an MNNTI, the CN 150 computes an MNN token from an MNNA 112 extracted from the MNNTI, together with KCN and a nonce.

[0059] Having generated tokens in response to the respective initialisation tests, the CN 150 performs the step 256 of sending a home address test (HoT) comprising a HoTI cookie, home nonce index and home token to the MR 120, and sending a care-of address test (CoT) comprising a CoTI cookie, care-of nonce index and care-of token to the MR 120, as known in the art. A nonce index allows the CN to retrieve the nonce used to generate a token, without sending the nonce itself as this would compromise security.

[0060] Additionally, the CN 150 sends a mobile network node address test (MNNT) comprising an MNNTI cookie, MNN nonce index and MNN token to the MNN 110, the MNNT further comprising;

a mobile router presence option (MRPO) that comprises the MR home address (HoA) 132.

[0061] The HoT is sent to the MR HoA 132, and the CoT is sent to the MR CoA 142. The MNNT is sent to the MNN address (MNNA) 112.

[0062] The intent is for the HoT and CoT to both reach the MR, and for the MNNT to reach the MNN.

[0063] Note that the MNN token will provide a more robust level of security within the validation process 200 if it remains confidential. To this end, a home agent (HA) 130 may encrypt an MNNT when tunnelling said MNNT to an MR 120 if the CN 150 does not encrypt it.

[0064] The mobile router presence option (MRPO) is an IP hop-by-hop option that instructs every router on the path to the recipient to examine it, although in practice only mobile routers will typically examine this option.

[0065] The inventors of the present invention have appreciated that this is necessary because the CN 150 addresses the MNNT to the MNN 110 to ensure it is routed to the correct place, but it is desired that the MR 120 - if it is the valid MR in the correct place - is able to intercept the MNNT, in order to generate a validation key with it. This requires the facility for the MR 120 to be able to examine some characterising portion of the MNNT, such as an MR HoA 132 within the MRPO.

[0066] Consequently the MR 120 compares its own home address 132 to an MR home address that it extracts from MNNTs that it receives for routing to the MNN 110.

[0067] In an alternative embodiment, the MRPO carries an MR care-of address (CoA) rather than an MR HoA, and the MR compares its own CoA 142 to an MR CoA that it extracts from MNNTs that it receives for routing to the MNN 110.

[0068] In the case of either HoA or CoA above, if the addresses match, the MR 120 does not forward the MNNT further to the MNN. Instead, it verifies that the MNNTI cookie extracted from the MNNT matches that sent by the MR 120 in the MNNTI, and upon verification of a match, extracts the MNN nonce index and MNN token from the MNNT.

[0069] The cookie thus provides a failsafe against maliciously constructed MNNTs.

[0070] The MR 120 is now in a position to generate a valid XBU.

[0071] Referring to FIG. 3, the MR 120, having received the MNNT, HoT and CoT, now possesses a home token, care-of token and MNN token generated by the CN 150. The MR is then able to generate a binding update validation key (KBM) 314 from the home token and care-of token that the CN 150 will recognise as belonging to the valid MR 120, as known in the art.

[0072] In addition, the MR 120 is also able to generate 266 an extended binding update (XBU) validation key (KBMNN) 324 from the MNN token.

[0073] In an embodiment of the present invention, the XBU is structured with the intent of being interpreted as a standard BU if received by a CN 150 incapable of understanding the extension.

[0074] The XBU is thus obtained by adding new options to the MIPv6 BU. The extended binding update thus comprises at least the following two options:

i. MNN address 320; and
ii. XBU signature 322.

[0075] An optional, yet preferred additional option iii. is the MNN nonce index 321.

[0076] The MNN address option 320 comprises the address of the MNN 112 for which the XBU is sent, whilst the XBU signature option 322 is generated 276 preferably based on a Message Authentication Code (MAC) that uses the KBMNN key 324, performed over the whole of the XBU.

[0077] The MR then sends the XBU to its recipient, typically the CN 150.

[0078] By incorporating a KBMNN key 324 based on the MNN token from the CN 150 in the signature 322, the CN 150 can validate a KBMNN based signature 322 extracted from an XBU 300 received by the CN 150 from the MR 120.

[0079] In an embodiment of the present invention, once the CN 150 has received and successfully validated an XBU 300, the CN 150 adds two entries to its binding cache (BC) derived from the validated XBU 300;

i. MR HoA 132 is marked as reachable though the MR CoA 142, as known in the art; and
ii. additionally, MNNA 112 is marked as reachable through the MR HoA 132.

[0080] One may assume that the CN uses recursive parsing of its binding cache, as detailed in EP 02291331.3 (Motorola).

[0081] Thus when the CN parses its BC with the MNN address 112 as the point of entry, the MR HoA 132 is first returned; due to recursive parsing of the BC, the MR HoA 132 is then searched in the BC, returning the MR CoA 142.

[0082] In an alternative embodiment of the present invention, the two entries added to the binding cache of the CN 150 are;

i. MR HoA 132 marked as reachable though the MR CoA 142, as known in the art; and
ii. additionally, MNNA 112 marked as reachable through the MR CoA 142.

[0083] Thus when the CN parses its BC with the MNN address 112 as the point of entry, the MR CoA 142 is first returned.

[0084] Then, in either embodiment, the CN 150 can then construct a packet with a single IP header whose destination is the first intermediate address, e.g. the MR CoA 142, followed by a routing header comprising other intermediate addresses such as the MR HoA 132 and the MNNA 112, and followed finally by the payload.

[0085] More generally in the case of nested mobile routers, the CN 150 will route packets for the MNN 110 with an IP header destination of the top-level mobile router care-of address, and with a routing header comprising at least the care-of addresses of subsequent mobile routers and the MNNA 112, followed finally by the payload.

[0086] It should be noted that if the CN 150 needs to refresh an expired MNN BC entry that was created in its binding cache (BC) by an XBU 300, then the CN 150 has to send a modified version of classical MIPv6 Binding Request message. That extended binding request (XBR) is sent to the MR and comprises the address 112 of the MNN 110 for which it is issued. Note that for purposes such as expiry and refreshment of data in the BC, one may distinguish the MNN BC entry ("MNN address is reachable at MR HoA") from the MR BC entry ("MR HoA is reachable at MR CoA") although both are created when CN 150 receives a validated XBU 300: typically, these two entries should not have the same lifetime (the lifetime of MNN BC entry is much longer). To enable the CN 150 to make this distinction, the structure of the CN BC should be slightly modified (for example by adding a flag for each entry specifying whether it is a MNN entry or not).

[0087] In an embodiment of the present invention, for the situation where a mobile router visits a mobile router (nested mobility), then a mobile router, upon receiving a tunnelled packet from its home agent, sends an XBU to the source address of the inner packet for the destination address of the inner packet.

[0088] Referring to parts 4A and 4B of FIG. 4, for the case of a first mobile router hosting a second mobile router:

[0089] A network of a first mobile router (MR1) 420 comprises a second mobile router (MR2) 460, and a network of MR2 460 comprises an MNN 410.

[0090] In order to compile a sequence of bindings in the CN binding cache that link the CN 150 to the MNN 110, the validation process 200 is instigated twice, first upon receipt of a first packet (FIG. 4A) by MR2 460 (tunnelled by MR2's HA 470), and second by receipt of a second packet (FIG. 4B) by MR1 420 (sent directly to the MR2 CoA 482 and tunnelled by MR1's HA 430). The encircled numbers in the FIGs 4A and 4B show the respective routes of the two packets.

[0091] Referring to Fig. 4A, upon receiving a first tunnelled packet MR1 420 sends an XBU 401 to the MR2's home agent (HA2) 470 for MR2 CoA 482, since HA2 address and MR2 CoA are respectively in the source and destination fields of the inner packet. (The inner packet being defined as beginning with the next IP header in a series within the packet; referring to FIG. 5, packet 510 commences with IP header 501, and its inner packet, also shown separately as 520, commences with header 502);

[0092] HA2 470 will typically ignore XBU 401; its purpose is to 'unwrap' the inner packet in a manner consistent with the validation process.

[0093] MR1 420 forwards the inner packet to MR2 460; MR2 460, upon receiving the packet, detunnels a (second) inner packet and sends an XBU 402 to CN 450 for MNNA 412, since CN and MNN addresses are respectively in the source and destination fields of the inner packet; MR2 460 finally forwards the inner packet to MNN 110.

[0094] The result is that CN updates its binding cache

to indirectly link the MNNA 112 with the MR2 CoA 482.

[0095] Referring to FIG. 4B, upon receiving a second tunnelled packed sent directly to MR2 CoA 482 with a routing header comprising the MR2 HoA 472 and MNNA 412, HA1 430 intercepts it and tunnels it to MR1 CoA 442.

[0096] Upon its receipt, MR1 420 sends an XBU 403 to CN 450 for MR2 CoA 482, since CN and MR2 Care-of addresses are respectively in the source and destination fields of the inner packet.

[0097] The result is that CN updates its binding cache to indirectly link the MR2 CoA 482 with the MR1 CoA 442.

[0098] Consequently, all the four entries thus generated in the CN BC, when parsed recursively, will route packets for the MNN 410 with an IP header destination of MR1 CoA 442, and with a routing header of {MR1 HoA 432, MR2 CoA 482, MR2 HoA 472, MNNA 412}.

[0099] It will be clear to a person skilled in the art that the above-described example is not limited to a single level of nesting of mobile networks.

[0100] In an enhanced embodiment of the present invention, for the situation where a mobile network visits a mobile network (nested mobility), there is an opportunity to avoid the sending of the first XBU 401 as described above. This has the added benefit that when *n* levels of mobile networks are nested, there is not a sequence of wasted XBUs. It also reduces the number of packets sent by the tunnelling method.

[0101] In this embodiment, a mobile router, upon receiving a tunnelled packet from its home agent, sends an XBU to the source address of the innermost packet for the destination address of the inner packet.

[0102] Referring to FIGs. 5 and 6, tunnelled packet 510 depicts a payload prepended with IP headers for each step of the route to the MNN. For simplicity, each IP header in packet 510 can be considered the header of a packet that comprises any subsequent packets and thus also the payload. Thus in this case the first packet 501 is addressed to MR1 CoA 442, whilst the innermost packet 506 is addressed to MNNA 112.

[0103] Upon receiving a first tunnelled packet 510, MR1 420 sends an XBU 516 to the source address of the innermost packet (CN) 512 for destination 514 of the second (or 'inner') packet 502, namely MR2 CoA 482.

[0104] This has the effect of enabling the CN to update its binding cache (BC) to link the MR1 CoA 442 to the MR2 CoA 482.

[0105] Passing the packet on to MR2 460, MR2 460 receives second packet 520. By repeating the above process, MR2 460 sends an XBU 526 to the source address of the innermost packet (CN) 522 for destination 524; an MR3 CoA, should it exist.

[0106] The process repeats until and including MRn, to which the MNN 410 is attached, is reached, when MRn sends an XBU 556 to the source address of the innermost packet CN 552 for the MNN 410.

[0107] The 2n entries thus generated in the CN BC, when parsed recursively, will route packets for the MNN 510 with an IP header destination of MR1 CoA 542. Note that in FIG. 6 the contents of the BC have been re-ordered for clarity of presentation.

[0108] For the case of the architecture illustrated in FIG 6 (which replicates that of FIGs 4A and 4B), a network of a first mobile router (MR1) 420 comprises a second mobile router (MR2) 460, a network of MR2 460 comprising an MNN 410.

upon receiving a first tunnelled packet, MR1 420 sends an XBU 601 to the source address of the innermost packet (CN) for MR2 CoA 482;
MR1 passes the packet to MR2 460.
upon receiving that packet, MR2 460 sends an XBU 602 to the source address of the innermost packet (CN) for MNN,

such that the four entries thus generated in the CN BC, when parsed recursively, will route packets for the MNN 410 with an IP header destination of MR1 CoA 442, and with a routing header of {MR1 HoA 432, MR2 CoA 482, MR2 HoA 472, MNNA 412}.

[0109] In an alternative embodiment of the present invention, a home address test initiation (HoTI) and mobile network node test initiation (MNNTI) may be combined, the resulting test initiation comprising a home/MNN TI cookie, MR HoA 132 and MNN address. It will be clear to a person skilled in the art that the processes described herein may readily be adapted to such a combined test initiation.

[0110] In a further alternative embodiment of the present invention, the MNNTI message is sent via the MR CoA 142.

[0111] In an alternative embodiment of the present invention, a care-of address test initiation (CoTI) and mobile network node test initiation (MNNTI) may be combined, the resulting test initiation comprising a care-of/MNN TI cookie, MR CoA 142 and MNN address. It will be clear to a person skilled in the art that the processes described herein may readily be adapted to such a combined test initiation.

[0112] In either of the above two alternative embodiments of the present invention, the MNNTI message sent via the MR CoA 142 may additionally comprise the MR HoA 132.

[0113] Apparatus for the role of correspondent node 150 may be any IP networkable appliance operable for use according to the methods described herein.

[0114] Apparatus for the role of mobile router 120 may be any IP networkable appliance capable of connecting a further IP networkable appliance operable for use according to the methods described herein.

Claims

1. A method of validated communication between a mobile network node, MNN, (110) and a correspondent node, CN, (150) via at least a first mobile router,

MR, (120), and **characterised by** the following steps :

i. employing a validation process (200) wherein an MNN test initiation, MNNTI, message is sent by the MR (120), and a MNN test, MNNT, message is sent by the CN (150); and
ii. sending from the MR (120) an extended binding update, XBU, comprising the MNN's address, MNNA, (112).

2. A method of validated communication according to claim 1, wherein
upon receipt of a tunnelled packet from a home agent, HA, (130) of the mobile router, MR, (120) addressed to the mobile network node, MNN, (110), the MR (120) initiates the validation process (200) between the MR (120) and correspondent node, CN, (150).

3. A method of validated communication according to any one of the preceding claims, wherein the validation process (200) between the mobile router, MR, (120) and correspondent node, CN, (150) comprises the step (226) of;
the MR (120) generating random values, hereinafter 'cookies', for a home address test initiation, HoTI, message and a care-of address test 4-nitiation, CoTI, message,
the method further comprising the step of
generating a cookie for the mobile network node test initiation, MNNTI, message.

4. A method of validated communication according to any one of the preceding claims, wherein the validation process (200) between the mobile router, MR, (120) and correspondent node, CN, (150) comprises the step (236) of;
the MR (120) sending a HoTI comprising the MR home address, HoA, (132) and a HoTI cookie to the CN (150); and
the MR (120) sending a CoTI comprising the MR care-of address, CoA, (142) and a CoTI cookie to the CN (150),
and
the MR (120) sending the MNNTI comprising the MNN address, MNNA, (112) and a MNNTI cookie to the CN (150).

5. A method of validated communication according to claim 4, wherein the HoTI is sent via the MR home address, HoA, (132), the CoTI is sent via the MR care-of address, CoA, (142) and the MNNTI is sent via either the HoA (132) or CoA (142).

6. A method of validated communication according to claim 5, wherein if the MNNTI is sent via the MR care-of address, COA, (142), the MNNTI message additionally comprises the MR home address, HoA, (132).

7. A method of validated communication according to any one of the preceding claims, wherein the validation process (200) between the mobile router, MR, (120) and correspondent node, CN, (150) comprises the step (246) of;
the CN (150) computing a home token from an HoA (132) extracted from a HoTI, a random key, KCN, and a nonce; and
the CN (150) computing a care-of token from a CoA (142) extracted from a CoTI, the KCN and a nonce, and
the CN (150) computing an MNN token from the MNNA (112) extracted from the MNNTI, the KCN and a nonce.

8. A method of validated communication according to any one of the preceding claims, wherein the validation process (200) between the mobile router, MR, (120) and correspondent node, CN, (150) comprises the step (256) of;
the CN (150) sending a home address test, HoT, comprising a HoTI cookie, home nonce index and home token to the MR (120); and
the CN (150) sending a care-of address test, CoT, comprising a CoTI cookie, care-of nonce index and care-of token to the MR (120),
and
the CN (150) sending the mobile network node address test, MNNT, comprising an MNNTI cookie, MNN nonce index and MNN token to the MNN (110), the MNNT further comprising;
a mobile router presence oPtion, MRPO, that comprises the MR home address, HoA, (132).

9. A method of validated communication according to any one of the preceding claims 1 to 7, wherein the validation process (200) between the mobile router, MR, (120) and correspondent node, CN, (150) comprises the step (256) of;
the CN (150) sending a home address test, HoT, comprising a HoTI cookie, home nonce index and home token to the MR (120); and
the CN (150) sending a care-of address test (CoT) comprising a CoTI cookie, care-of nonce index and care-of token to the MR (120),
and
the CN (150) sending the mobile network node address test, MNNT, comprising an MNNTI cookie, MNN nonce index and MNN token to the MNN (110), the MNNT further comprising;
a mobile router presence option, MRPO, that comprises the care-of address, CoA, (142).

10. A method of validated communication according to any one of claims 8 and 9, wherein the HoT is sent

to the MR home address, HoA, (132), the CoT is sent to the MR care-of address, CoA, (142) and the MNNT is sent to the MNN address, MNNA, (112).

11. A method of validated communication according to any one of the preceding claims, wherein the validation process (200) between the mobile router, MR, (120) and correspondent node, CN, (150) comprises the step of :

a home agent, HA, (130) encrypting the MNNT when tunnelling said MNNT to an MR (120).

12. A method of validated communication according to any one of the preceding claims, wherein the validation process (200) between the mobile router, MR, (120) and correspondent node, CN, (150) comprises the step of : the MR (120) comparing its own home address (132) to
the MR (120) comparing its own home address (132) to any MR home address that the MR (120) can extract from MNNTs that it receives for routing to the MNN (110).

13. A method of validated communication according to any one of the preceding claims, wherein the validation process (200) between the mobile router, MR, (120) and correspondent node, CN, (150) comprises the step of :

the MR (120) comparing its own care-of address (142) to any CoA that the MR (120) can extract from MNNTs that it receives for routing to the MNN (110).

14. A method of validated communication according to any one of claims 12 and 13, wherein if the addresses match,
the MR (120) does not forward the MNNT further; verifies that an MNNTI cookie extracted from the MNNT matches that sent by the MR (120) in the MNNTI; and
upon verification of a match, extracts the MNN nonce index and MNN token from the MNNT.

15. A method of validated communication according to any one of the preceding claims, wherein the validation process (200) between the mobile router (MR) (120) and correspondent node (CN) (150) comprises the step (266) of;
the MR (120) generating an extended binding update (XBU) validation key, KBMNN, (324) from the MNN token.

16. A method of validated communication according to any one of the preceding claims, wherein the validation process (200) between the mobile router, MR, (120) and correspondent node, CN, (150) comprises the step (276) of;
the MR (120) generating an extended binding update XBU, signature (322) using a KBMNN key (324).

17. A method according to claim 16 wherein the signature is based upon a message authentication code using the KBMNN key (324).

18. A method of validated communication according to any one of the preceding claims, wherein the extended binding update comprises at least two options:

i. MNN address (320); and
ii. XBU signature (322).

19. A method of validated communication according to claim 18 wherein the extended binding update further comprises an MNN nonce index option (321).

20. A method of validated communication according to any one of the preceding claims, wherein the validation process (200) between the mobile router, MR, (120) and correspondent node, CN, (150) comprises the step of :

the CN (150) validating a KBMNN based signature (322) extracted from an XBU (300) received by the CN (150) from the MR (120).

21. A method of validated communication according to any one of the preceding claims, wherein the validation process (200) between the mobile router, MR, (120) and correspondent node, CN, (150) comprises the step of;
the CN (150) adding two entries to its binding cache (BC) derived from a validated XBU (300);

i. MR HoA (132) is marked as reachable though the MR CoA (142) ; and
ii. MNNA (112) is marked as reachable through the MR HoA (132).

22. A method of validated communication according to any one of the preceding claims, wherein the validation process (200) between the mobile router, MR, (120) and correspondent node, CN, (150) comprises the step of :

the CN (150) adding two entries to its binding cache (BC) derived from a validated XBU (300);

i. MR HoA (132) is marked as reachable though the MR CoA (142); and
ii. MNNA (112) is marked as reachable through the MR CoA (142).

23. A method of validated communication according to any one of claims 21 and 22, wherein if the MNN 110

is the addressee, the CN (150) recursively parses its BC,
and such that the CN (150) will route packets for the MNN (110) with an IP header destination of MR CoA (142), and with a routing header comprising at least MNNA (412).

24. A method of validated communication according to any one of claims 21 and 22, wherein if the MNN (110) is the addressee under at least two nested mobile routers, then the CN (150) recursively parses its BC,
and such that the CN (150) will route packets for the MNN 110 with an IP header destination of the top-level mobile router care-of address, and with a routing header comprising at least the care-of addresses of subsequent mobile routers and the MNNA (112).

25. A method of validated communication according to any one of claims 2 to 23, wherein the mobile router, MR, (120) only initiates the validation process 200 between the MR (120) and correspondent node, CN, (150) if at least one of the following set of conditions is met;

i. the MNNA (110) subscribes to a specified service;
ii. the CN (150) has not ignored a threshold number of prior XBUs (300);
iii. the CN (150) has not ignored a threshold number of validation processes; and
iv. the MNNA (110) satisfies a usage policy.

26. A method of validated communication according to any one of claims 3 to 25, wherein the home address test initiation, HoTI, and mobile network node test initiation , MNNTI, are combined, the resulting test initiation comprising a home/MNN TI cookie, MR HoA (132) and MNN address (112).

27. A method of validated communication according to any one of claims 3 to 25, wherein the care-of address test initiation, CoTI, and mobile network node test initiation, MNNTI are combined, the resulting test initiation comprising a care-of/MNN TI cookie, MR CoA (142) and MNN address (112).

28. A method of validated communication according to any one of the preceding claims, the method further comprising the following step;
the mobile router, MR, 120, upon receiving a tunnelled packet from its home agent, HA, 130, sends an XBU 300 to the source address of an inner packet for a destination address of the inner packet.

29. A method of validated communication according to claim 28, wherein a network of a first mobile router, MR1, (420) comprises a second mobile router, MR2, (460), the network of MR2 (460) comprising an MNN (410), the method comprising the following steps;
upon receiving a first tunnelled packet MR1 (420) sends an XBU (401) to the MR2's home agent, HA2, (470) for MR2 CoA (482);
MR1 (420) forwards an inner packet to MR2 (460);
MR2 (460) upon receiving the packet sends and XBU (402) to CN (450) for MNNA (412);
upon receiving a second tunnelled packed sent directly to MR2 CoA (482) with a routing header comprising the MR2 HoA (472) and MNNA (412), HA1 (430) intercepts it and tunnels an inner packet to MR1 CoA (442); and
MR1 (420) upon receiving the packet sends an XBU (403) to CN (450) for MR2 CoA (482),
and such that the four entries thus generated in the CN BC, when parsed recursively, will route packets for the MNN (410) to with an IP header destination of MR1 CoA (442), and with a routing header of MR1 HoA (432), MR2 CoA (482), MR2 HoA (472), MNNA (412).

30. A method of validated communication according to any one of claims 1 to 27, the method further **characterised by** the following step;
the mobile router, MR, 120, upon receiving a tunnelled packet from its home agent, HA, 130, sends an XBU 300 to a source address of an innermost packet for a destination address of the inner packet.

31. A method of validated communication according to claim 30, wherein a network of a first mobile router, MR1, (420) comprises a second mobile router, MR2, (460), the network of MR2 (460) comprising an MNN (410), comprising the following steps;
upon receiving a first tunnelled packet, MR1 (420) sends an XBU (601) to the source address of the innermost packet, CN, for MR2 CoA (482);
MR1 (520) passes the inner packet to MR2 (460),
upon receiving the inner packet, MR2 (460) sends an XBU (602) to the source address of the innermost packet (CN) for MNN,
and such that the four entries thus generated in the CN BC, when parsed recursively, will route packets for the MNN (510) with an IP header destination of MR1 CoA. (542), and with a routing header of, MR1 HoA (532), MR2 CoA (582), MR2 HoA (572), MNNA (512).

32. Apparatus for use in a validated communication according to a method as claimed in any one of claims 1 to 31, between a mobile network node, MNN, (110) and a correspondent node, CN, (150) via at least a first mobile router, MR, (120), and comprising:

i. checking means for performing a validation process (200) wherein the MNN test initiation, MNNTI, message is sent by the MR 120, and a

MNN test, MNNT, message is sent by the CN (150); and
ii. extended binding update means for sending (276) from the MR (120) an extended binding update (XBU) comprising the MNN's address, MNNA, (112).

33. A mobile router, MR, (120) for connection with at least one further IP networkable appliance in communication by a method as claimed in any one of claims 1 to 31, the MR (120) comprising mobile network node, MNN, test initiation, MNNTI, message means for generating and sending a MNNTI message, and binding update means for generating and sending an extended binding update, XBU, (300) comprising the MNN's address, MNNA, (112).

34. A correspondent node, CN, (150) for connection with at least one IP networkable appliance in communication by a method as claimed in any one of claims 1 to 31, the CN (120) comprising mobile network node, MNN, test, MNNT, message means for generating and sending a, MNNT message, and validation means for validating an extended binding update validation key, KBMNN, based signature (322) extracted from an extended binding update, XBU, (300).

Patentansprüche

1. Verfahren zur validierten Kommunikation zwischen einem mobilen Netzknoten, MNN, (110) und einem entsprechenden bzw. Korrespondenz-Knoten, CN, (150) über zumindest einen ersten mobilen Router, MR, (120), wobei das Verfahren durch die folgenden Schritte **gekennzeichnet** ist:

i. Verwendung eines Validierungsprozesses (200), wobei eine MNN-Testeinleitungs-, MNNTI, -Nachricht von dem mobilen Router MR (120) gesendet wird, und wobei eine MNN-Test-, MNNT, -Nachricht von dem Korrespondenz-Knoten CN (150) gesendet wird; und
ii. Sendung von dem mobilen Router (120) einer erweiterten Binding Update bzw. Bindungsaktualisierung, XBU, welche die MNN-Adresse, MNNA, (112) aufweist.

2. Verfahren zur validierten Kommunikation gemäß Anspruch 1, **dadurch gekennzeichnet, dass** nach Empfang eines an den mobilen Netzwerkknoten, MNN, (110) adressierten getunneltes Datenpakets von einem Heimat-Agenten, HA, (130) des mobilen Routers (110), der mobile Router MR (120) den Validierungsprozess (200) zwischen dem MR (120) und dem Korrespondenz-Knoten, CN, (150) einleitet.

3. Verfahren zur validierten Kommunikation nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** der Validierungsprozess (200) zwischen dem mobilen Router, MR, (120) und dem Korrespondenz-Knoten CN (150) den folgenden Schritt aufweist:

der MR (120) erzeugt Zufallswerte, nachfolgend "Cookies" genannt, für eine Heimatadressen-Testeinleitungs-, HoTI, -Nachricht sowie für eine Care-of- Adressen-Testeinleitungs-, Co-TI, -Nachricht, wobei das Verfahren des Weiteren den folgenden Schritt aufweist:

Erzeugung eines Cookies für die mobile Netzknoten-Testeinleitungs-, MNNTI, -Nachricht.

4. Verfahren zur validierten Kommunikation nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** der Validierungsprozess (200) zwischen dem mobilen Router, MR, (120) und dem Korrespondenz-Knoten, CN, (150) den folgenden Schritt (236) aufweist:

der MR (120) sendet eine HoTI, welche die MR-Heitmatadresse, HoA, (132) sowie ein HoTI-Cookie aufweist, an den Korrespondenz-Knoten CN (150); und
der MR (120) sendet eine CoTI, welche die MR-Care-of-Adresse, CoA, (142) sowie ein CoTI-Cookie aufweist, an den CN (150); und
der MR (120) sendet die MNNTI, welche die MNN-Adresse, MNNA, (112) sowie ein MNNTI-Cookie aufweist, an den CN (150).

5. Verfahren zur validierten Kommunikation nach Anspruch 4, **dadurch gekennzeichnet, dass** die HoTI über die MR-Heimatadresse, HoA, (132), die CoTI über die MR-Care-of-Adresse, CoA, (142) und die MNNTI über entweder die HoA (132) oder die CoA (142) gesendet wird.

6. Verfahren zur validierten Kommunikation nach Anspruch 5, **dadurch gekennzeichnet, dass** wenn die MNNTI über die MR-Care-of-Adresse, CoA, (142) gesendet wird, die MNNTI-Adresse zusätzlich die MR-Heimatadresse, HoA, (132) aufweist.

7. Verfahren zur validierten Kommunikation nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** der Validierungsprozess (200) zwischen dem mobilen Router, MR, (120) und dem Korrespondenz-Knoten, CN, (150) den folgenden Schritt (246) aufweist:

der CN (150) berechnet ein Heimatmerkmal aus einer aus einer HoTI extrahierten HoA (132), ei-

nem Zufallsschlüssel, KCN, und einer Nonce; und
der CN (150) berechnet ein Care-of-Merkmal aus einer aus einer CoTI extrahierten CoA (142), dem KCN und einer Nonce; und
der CN (150) berechnet ein MNN-Merkmal aus der aus der MNNTI extrahierten MNNA (112), dem KCN und einer Nonce.

8. Verfahren zur validierten Kommunikation nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** der Validierungsprozess (200) zwischen dem mobilen Router, MR, (120) und dem Korrespondenz-Knoten, CN, (150) den folgenden Schritt (256) aufweist:

der CN (150) sendet einen Heimatadressen-Test, HoT, welcher ein HoTI-Cookie, einen Heimat Nonce Index sowie ein Heimatmerkmal aufweist, an den MR (120); und
der CN (150) sendet einen Care-of-Adressen-Test, CoT, welcher ein CoTI-Cookie, einen Care-of-Nonce Index sowie ein Care-of-Merkmal aufweist, an den MR (120); und
der CN (150) sendet den mobilen Netzknotenadressen-Test MNNT, welcher ein MNNTI-Cookie, einen MNN-Nonceindex sowie ein MNN-Merkmal aufweist, an den MNN (110), wobei der MNNT des Weiteren Folgendes aufweist:

eine Anwesenheitsoption für den mobilen Router, MRPO, welche die MR-Heimatadresse HOA (132) aufweist.

9. Verfahren zur validierten Kommunikation nach einem der Ansprüche 1 bis 7, **dadurch gekennzeichnet, dass** der Validierungsprozess (200) zwischen dem mobilen Router, MR, (120) und dem Korrespondenz-Knoten, CN, (150) den folgenden Schritt (256) aufweist:

der CN (150) sendet einen Heimatadressen-Test, HoT, welcher ein HoTI-Cookie, einen Heimat Nonce Index sowie ein Heimatmerkmal aufweist, an den MR (120); und
der CN (150) sendet einen Care-of-Adressen-Test, CoT, welcher ein CoTI-Cookie, einen Care-of-Nonce Index sowie ein Care-of-Merkmal aufweist, an den MR (120); und
der CN (150) sendet den mobilen Netzknotenadressen-Test, MNNT, welcher ein MNNTI-Cookie, einen MNN-Nonce Index sowie ein MNN-Merkmal aufweist, an den MNN (110), wobei der MNNT des Weiteren Folgendes aufweist:

eine Anwesenheitsoption für den mobilen Router, MRPO, welche die Care-of-Adresse, CoA, (142) aufweist.

10. Verfahren zur validierten Kommunikation gemäß einem der Ansprüche 8 und 9, **dadurch gekennzeichnet, dass** der HoT an die MR-Heimatadresse, HoA, (132), der CoT an die MR-Care-of-Adresse, CoA, (142) und der MNNT an die MNN-Adresse, MNNA, (112) gesendet wird.

11. Verfahren zur validierten Kommunikation gemäß einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** der Validierungsprozess (200) zwischen dem mobilen Router, MR, (120) und dem Korrespondenzknoten, CN, (150) den folgenden Schritt aufweist:

ein Heimat-Agent,HA, (130) verschlüsselt den MNNT, wenn der MNNT an einen MR (120) getunnelt wird.

12. Verfahren zur validierten Kommunikation nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** der Validierungsprozess (200) zwischen dem mobilen Router, MR, (120) und dem Korrespondenz-Knoten, CN, (150) den folgenden Schritt aufweist:

der MR (120) vergleicht seine eigene Heimat-Adresse (132) mit jeder beliebigen MR-Heimatadresse, welche der MR (120) aus MNNTs, welche er zum Routen bzw. Weiterleiten der MNN (110) empfängt, extrahieren kann.

13. Verfahren zur validierten Kommunikation gemäß einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** der Validierungsprozess (200) zwischen dem mobilen Router, MR, (120) und dem Korrespondenz-Knoten ,CN, (150) den folgenden Schritt aufweist:

der MR (120) vergleicht seine eigene Care-of-Adresse (142) mit jeder beliebigen CoA, welche der MR (120) aus MNNTs, welche er zum Routen bzw. Steuern des MNN (110) empfängt, extrahieren kann.

14. Verfahren zur validierten Kommunikation gemäß einem der Ansprüche 12 und 13, **dadurch gekennzeichnet, dass** wenn die Adressen übereinstimmen,
der MR (120) den MNNT nicht weiterleitet;
prüft bzw. bestätigt, dass ein MNNTI-Cookie, welches aus dem MNNT extrahiert wird, mit dem von dem MR (120) in der MNNTI gesendeten Cookie übereinstimmt; und
nach der Verifizierung einer Übereinstimmung den MNN-Nonce Index und das MNN-Merkmal aus dem MMNT extrahiert.

15. Verfahren zur validierten Kommunikation gemäß einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** der Validierungsprozess (200) zwischen dem mobilen Router, MR, (120) und dem Korrespondenz-Knoten, CN, (150) den folgenden Schritt aufweist:

der MR (120) erzeugt einen erweiterten Binding Update- bzw. Bindungsaktualisierungs-, XBU,-Validierungsschlüssel, KBMNN, (324) aus dem MNN-Merkmal.

16. Verfahren zur validierten Kommunikation gemäß einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** der Validierungsprozess (200) zwischen dem mobilen Router, MR, (120) und dem Korrespondenz-Knoten, CN, (150) den folgenden Schritt (276) aufweist:

der MR (120) erzeugt eine erweiterte Binding Update- bzw. Bindungsaktualisierungs-, XBU,-Signatur (322) unter Verwendung des KBMNN-Schlüssels (324).

17. Verfahren nach Anspruch 16, **dadurch gekennzeichnet, dass** die Signatur auf einem Nachrichten-Authentifizierungscode beruht, welcher den KBMNN-Schlüssel (324) verwendet.

18. Verfahren zur validierten Kommunikation gemäß einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** die erweiterte Bindungsaktualisierung mindestens zwei Optionen aufweist:

i. eine MNN-Adresse (320); und
ii. eine XBU-Signatur (322).

19. Verfahren zur validierten Kommunikation gemäß Anspruch 18, **dadurch gekennzeichnet, dass** die erweiterte Bindungsaktualisierung des Weiteren eine MNN-NonceIndex-Option (321) aufweist.

20. Verfahren zur validierten Kommunikation nach einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** der Validierungsprozess (200) zwischen dem mobilen Router MR (120) und dem Korrespondenz-Knoten, CN, (150) den folgenden Schritt aufweist:

der CN (150) validiert eine von einer XBU (300) extrahierte KBMNNbasierende Signatur (322), wobei die XBU (300) durch den CN (150) von dem MR (120) empfangen wird.

21. Verfahren zur validierten Kommunikation gemäß einem der vorhergehenen Ansprüche, **dadurch gekennzeichnet, dass** der Validierungsprozess (200) zwischen dem mobilen Router, MR, (120) und dem Korrespondenz-Knoten ,CN, (150) den folgenden Schritt aufweist:

der CN (150) addiert zwei Eingänge bzw. Einträge in seinen Bindungs-Zwischenspeicher (BC), welche von zur validierten XBU (300) erhalten bzw. abgeleitet werden;

i. die MR-HoA (132) wird durch die MR-CoA (142) als erreichbar markiert; und
ii. die MNNA (112) wird durch die MR-HoA (132) als erreichbar markiert.

22. Verfahren zur validierten Kommunikation gemäß einem der vorhergehenden Ansprüche, **dadurch gekennzeichnet, dass** der Validierungsprozess (200) zwischen dem mobilen Router, MR, (120) und dem Korrespondenz-Knoten, CN, (150) den folgenden Schritt aufweist:

der CN (150) addiert zwei Eingänge bzw. Einträge in seinen Bindungs-Zwischenspeicher (BC), welche sich von einer validierten XBU (300) ableiten;

i. die MR-HoA (132) wird durch die MR-CoA (142) als erreichbar markiert; und
ii. die MNNA (112) wird durch die MR-CoA (142) als erreichbar markiert.

23. Verfahren zur validierten Kommunikation gemäß einem der Ansprüche 21 und 22, **dadurch gekennzeichnet, dass** der MNN (110) der Adressat bzw. Empfänger ist, der CN (150) seinen Bindungs-Zwischenspeicher BC rekursiv parst bzw. analysiert, und so dass der CN (150) Datenpakete für den MNN (110) mit einem IP-Datenkopfziel MR-CoA (142) sowie mit einem Routing-Datenkopf, welcher zumindest die MNNA (412) aufweist, routet bzw. weiterleitet.

24. Verfahren zur validierten Kommunikation gemäß einem der Ansprüche 21 und 22, **dadurch gekennzeichnet, dass** falls der MNN (110) der Adressat unter mindestens zwei verschachtelten Routern ist, der CN (150) dann seinen Bindungs-Zwischenspeicher BC rekursiv parst bzw. analysiert, und so dass der CN (150) Datenpakete für den MNN 110 mit einem IP-Datenkopfziel der mobilen Router-Spitzen-Care-of-Adresse und mit einem Routing-Datenkopf, welcher zumindest die Care-of-Adressen nachfolgender mobiler Router und die MNNA (112) aufweist, routet bzw. weiterleitet.

25. Verfahren zur validierten Kommunikation gemäß einem der Ansprüche 2 bis 23, **dadurch gekennzeichnet, dass** der mobile Router, MR, (120) nur den Validierungsprozess (200) zwischen dem MR

(120) und dem Korrespondenz-Knoten, CN, (150) einleitet, falls mindestens eine der nachfolgenden Gruppen von Bedingungen erfüllt wird;

i. der MNN (110) nimmt an einem spezifischen Dienst teil;
ii. der CN (150) hat keine Schwellenanzahl früherer XBUs (300) missachtet;
iii. der CN (150) hat keine Schwellenanzahl von Validierungsprozessen missachtet; und
iv. der MNN (110) erfüllt eine Nutzungs-Richtlinie.

26. Verfahren zur validierten Kommunikation gemäß einem der Ansprüche 3 bis 25, **dadurch gekennzeichnet, dass** die Heimatadressen-Testeinleitung, HoTI, und die mobile Netzknoten-Testeinleitung, MNNTI, kombiniert werden, wobei die resultierende Testeinleitung ein Heimat/MNN TI-Cookie, eine MR-HoA (132) sowie eine MNN-Adresse (112) aufweist.

27. Verfahren zur validierten Kommunikation gemäß einem der Ansprüche 3 bis 25, **dadurch gekennzeichnet, dass** die Care-of-Adressen-Testeinleitung, CoTI, und die mobile Netzknoten-Testeinleitung, MNNTI, kombiniert werden, wobei die resultierende Testeinleitung ein Care-of/MNN TI-Cookie, eine MR-CoA (142) sowie eine MNN-Adresse (112) aufweist.

28. Verfahren zur validierten Kommunikation gemäß einem der vorhergehenden Ansprüche, wobei das Verfahren des Weiteren den folgenden Schritt aufweist:

der mobile Router, MR, (120) sendet nach Empfang eines getunnelten Datenpakets von seinem Heimat-Agenten, HA, (130) eine XBU 300 an die Ursprungsadresse eines inneren Datenpakets für eine Zieladresse des inneren Datenpakets.

29. Verfahren zur validierten Kommunikation gemäß Anspruch 28, **dadurch gekennzeichnet, dass** ein Netzwerk eines ersten mobilen Routers, MR1, (420) einen zweiten mobilen Router MR2 (460) aufweist, wobei das Netzwerk des MR2 (460) einen MMN (410) aufweist, wobei das Verfahren die folgenden Schritte einschließt:

nach Empfang eines ersten getunnelten Datenpakets, sendet MR1 (420) eine XBU (401) an den MR2-Heimat-Agenten, HA2, (470) für MR2-CoA (482);
MR1 (420) leitet ein inneres Datenpaket weiter an MR2 (460);
MR2 (460) sendet nach Empfang des Datenpakets eine XBU (402) an den CN (450) für eine MNNA (412);
nach Empfang eines zweiten getunnelten Datenpakets, welches direkt an die MR2-CoA (482) mit einem Routing-Datenkopf gesendet wird, welcher die MR2-HoA (472) und die MNNA (412) aufweist, fängt der HA1 (430) dieses ab und tunnelt ein inneres Datenpaket an die MR1-CoA (442); und
MR1 (420) sendet nach Empfang des Datenpakets eine XBU (403) an den CN (450) für eine MR2-CoA (482),
und so dass die vier auf diese Weise in dem CN-Bindungs-Zwischenspeicher CN-BC erzeugten Einträge bzw. Eingänge bei rekursivem Analysieren bzw. Parsen, Datenpakete für den MNN (410) mit einem IP-Datenkopf-Ziel von MR1-CoA (442), und mit einem Routing-Datenkopf von MR1-HoA (432), MR2-CoA (482), MR-HoA (472), MNNA (412) routen bzw. weiterleiten.

30. Verfahren zur validierten Kommunikation gemäß einem der Ansprüche 1 bis 27, wobei das Verfahren des Weiteren durch den folgenden Schritt **gekennzeichnet** ist:

der mobile Router, MR, (120) sendet nach Empfang eines getunnelten Datenpakets von seinem Heimat-Agenten HA (130) eine XBU 300 an eine Ursprungsadresse eines innersten Datenpakets für eine Zieladresse des inneren Datenpakets.

31. Verfahren zur validierten Kommunikation gemäß Anspruch 30, **dadurch gekennzeichnet, dass** ein Netzwerk eines ersten mobilen Routers, MR1, (420) einen zweiten mobilen Router MR2 (460) aufweist, wobei das Netzwerk von MR2 (460) einen MNN (410) aufweist, wobei das Verfahren die folgenden Schritte einschließt:

nach Empfang eines ersten getunnelten Datenpakets sendet MR1 (420) eine XBU (601) an die Ursprungsadresse des innersten Datenpakets CN für MR2-CoA (482);
MR1 (520) leitet das innere Datenpaket zu MR2 (460) weiter;
nach Empfang des inneren Datenpakets sendet MR2 (460) eine XBU (602) an die Ursprungsadresse des innersten Datenpakets CN für den MNN,
und so dass die vier auf diese Weise in dem CN-BC erzeugten Einträge bzw. Eingaben bei rekursivem Analysieren bzw. Parsen Datenpakete für den MNN (510) mit einem IP-Datenkopfziel der MR1-CoA (542) und mit einem Routing-Datenkopf der MR1-HoA (532), der MR2-CoA (582), der MR2-HoA (572), der MNNA (512) routen.

32. Verfahren zur Verwendung in einer validierten Kommunikation gemäß einem Verfahren nach einem der Ansprüche 1 bis 31 zwischen einem mobilen Netzknoten, MNN, (110) und einem Korrespondenz-Knoten, CN, (150) über mindestens einen ersten mobilen Router, MR, (120), und wobei wobei das Verfahren Folgendes aufweist:

i. eine Prüfeinrichtung zur Ausführung eines Validierungsprozesses (200), wobei die MNN-Testeinleitungs-, MMNTI, -Nachricht durch den MR (120) gesendet wird, und wobei eine MNN-Test-, MNNT, -Nachricht von dem CN (150) gesendet wird; und
ii. eine Einrichtung zur erweiterten Bindungsaktualisierung zum Senden (276) einer erweiterten Bindungsaktualisierung (XBU), welche die MNN-Adresse, MNNA, (112) aufweist, von dem MR (120).

33. Mobiler Router, MR, (120) zur Verbindung mit mindestens einem weiteren IP-netzwerkfähigen Gerät, welches durch ein Verfahren gemäß einem der Ansprüche 1 bis 31 in Kommunikation steht, wobei der MR (120) eine mobile Netzknoten-,MNN, -Testeinleitungs-,MNNTI,-Nachrichten-Einrichtung zum Erzeugen und Senden einer MNNTI-Nachricht sowie eine Bindungaktualisierungs-Einrichtung zum Erzeugen und Senden einer erweiterten Bindungsaktualisierung, XBU, (300), welche die MNN-Adresse, MNNA, aufweist, aufweist.

34. Korrespondenz-Knoten, CN, (150) zur Verbindung mit mindestens einem IP-netzwerkfähigen Gerät, welches durch ein Verfahren gemäß einem der Ansprüche 1 bis 31 in Kommunikation steht, wobei der CN (150) eine mobile Netzknoten-,MNN,-Test-, MNNT-Nachrichten-Einrichtung zum Erzeugen und Senden einer MNNT-Nachricht sowie eine Validierungseinrichtung zur Validierung einer aus einer erweiterten Bindungsaktualisierung XBU (300) extrahierten Signatur (322) auf der Basis eines erweitereten Bindungsaktualisierungs-Validierungsschlüssels KBMNN.

Revendications

1. Procédé de communication validée entre un noeud de réseau mobile, MNN, (110) et un noeud correspondant, CN, (150) via au moins un premier routeur mobile, MR, (120), et **caractérisé par** les étapes ci-dessous consistant à:

i. employer un processus de validation (200) dans lequel un message d'initiation de test de noeud MNN, MNNTI, est envoyé par le routeur MR (120), et un message de test de noeud MNN, MNNT, est envoyé par le noeud CN (150) ; et
ii. envoyer, à partir du routeur MR (120), une mise à jour obligatoire étendue, XBU, comportant l'adresse de noeud MNN, MNNA, (112).

2. Procédé de communication validée selon la revendication 1, dans lequel:

suite à la réception d'un paquet mis sous tunnel par un agent domestique, HA, (130) du routeur mobile, MR, (120) adressé au noeud de réseau mobile, MNN, (110), le routeur MR (120) initie le processus de validation (200) entre le routeur MR (120) et le noeud correspondant, CN, (150).

3. Procédé de communication validée selon l'une quelconque des revendications précédentes, dans lequel le processus de validation (200) entre le routeur mobile, MR, (120) et le noeud correspondant, CN, (150) comporte l'étape ci-dessous (226) dans laquelle:

le routeur MR (120) génère des valeurs aléatoires ci-après appelées « témoins » pour un message d'initiation de test d'adresse domestique, HoTI, et un message d'initiation de test d'adresse au bon soin, COTI;
le procédé comportant en outre l'étape ci-dessous consistant à:

générer un témoin pour le message d'initiation de test de noeud de réseau mobile, MNNTI.

4. Procédé de communication validée selon l'une quelconque des revendications précédentes, dans lequel le processus de validation (200) entre le routeur mobile, MR, (120) et le noeud correspondant, CN, (150) comporte l'étape ci-dessous (236) dans laquelle:

le routeur MR (120) envoie une initiation HoTI comportant l'adresse domestique de routeur MR, HoA, (132) et un témoin d'initiation HoTI au noeud CN (150); et
le routeur MR (120) envoie une initiation COTI comportant l'adresse au bon soin de routeur MR, CoA, (142) et un témoin d'initiation CoTI au noeud CN (150); et
le routeur MR (120) envoie l'initiation MNNTI comportant l'adresse de noeud MNN, MNNA, (112) et un témoin d'initiation MNNTI au noeud CN (150).

5. Procédé de communication validée selon la revendication 4, dans lequel l'initiation HoTI est envoyée via l'adresse domestique de routeur MR, HoA, (132), l'initiation CoTI est envoyée via l'adresse au bon soin

de routeur MR, CoA, (142) et l'initiation MNNTI est envoyée via l'adresse HoA (132) ou l'adresse CoA (142).

6. Procédé de communication validée selon la revendication 5, dans lequel si l'initiation MNNTI est envoyée via l'adresse au bon soin de routeur MR, CoA, (142), le message d'initiation MNNTI comporte en outre l'adresse domestique de routeur MR, HoA, (132).

7. Procédé de communication validée selon l'une quelconque des revendications précédentes, dans lequel le processus de validation (200) entre le routeur mobile, MR, (120) et le noeud correspondant, CN, (150) comporte l'étape ci-dessous (246) dans laquelle:

le noeud CN (150) calcule un jeton domestique à partir d'une adresse HoA (132) extraite d'une initiation HoTI, une clé aléatoire, KCN, et une valeur à usage unique; et
le noeud CN (150) calcule un jeton au bon soin à partir d'une adresse CoA (142) extraite d'une initiation CoTI, la clé KCN et une valeur à usage unique; et
le noeud CN (150) calcule un jeton de noeud MNN à partir de l'adresse MNNA (112) extraite de la MNNTI, la KCN et une valeur à usage unique.

8. Procédé de communication validée selon l'une quelconque des revendications précédentes, dans lequel le processus de validation (200) entre le routeur mobile, MR, (120) et le noeud correspondant, CN, (150) comporte l'étape ci-dessous (256) dans laquelle:

le noeud CN (150) envoie un test d'adresse domestique, HoT, comportant un témoin d'initiation HoTI, un index de valeur à usage unique domestique et un jeton domestique au routeur MR (120) ; et
le noeud CN (150) envoie un test d'adresse au bon soin, CoT, comportant un témoin d'initiation CoTI, un index de valeur à usage unique au bon soin et un jeton au bon soin au routeur MR (120); et
le noeud CN (150) envoie le test d'adresse de noeud de réseau mobile, MNNT, comportant un témoin de MNNTI, un index de valeur à usage unique de noeud MNN et un jeton de noeud MNN au noeud MNN (110), le test MNNT comportant en outre:

une option de présence de routeur mobile, MRPO, laquelle comporte l'adresse domestique de routeur MR (132).

9. Procédé de communication validée selon l'une quelconque des revendications précédentes 1 à 7, dans lequel le processus de validation (200) entre le routeur mobile, MR, (120) et le noeud correspondant, CN, (150) comporte l'étape ci-dessous (256) dans laquelle:

le noeud CN (150) envoie un test d'adresse domestique, HoT, comportant un témoin d'initiation HoTI, un index de valeur à usage unique domestique et un jeton domestique au routeur MR (120); et
le noeud CN (150) envoie un test d'adresse au bon soin (CoT) comportant un témoin d'initiation CoTI, un index de valeur à usage unique au bon soin et un jeton au bon soin au routeur MR (120); et
le noeud CN (150) envoie le test d'adresse de noeud de réseau mobile, MNNT, comportant un témoin d'initiation MNNTI, un index de valeur à usage unique de noeud MNN et un jeton de noeud MNN au noeud MNN (110), le test MNNT comportant en outre:

une option de présence de routeur mobile, MRPO, laquelle comporte l'adresse au bon soin, CoA, (142).

10. Procédé de communication validée selon l'une quelconque des revendications 8 et 9, dans lequel le test HoT est envoyé à l'adresse domestique de routeur MR, HoA, (132), le test CoT est envoyé à l'adresse au bon soin de routeur MR, CoA, (142) et le test MNNT est envoyé à l'adresse de noeud MNN, MNNA, (112).

11. Procédé de communication validée selon l'une quelconque des revendications précédentes, dans lequel le processus de validation (200) entre le routeur mobile, MR, (120) et le noeud correspondant, CN, (150) comporte l'étape ci-dessous dans laquelle:

un agent domestique, HA, (130) chiffre le test MNNT lors de la mise sous tunnel dudit test MNNT vers un routeur MR (120).

12. Procédé de communication validée selon l'une quelconque des revendications précédentes, dans lequel le processus de validation (200) entre le routeur mobile, MR, (120) et le noeud correspondant, CN, (150) comporte l'étape ci-dessous dans laquelle:

le routeur MR (120) compare sa propre adresse domestique (132) à une quelconque adresse domestique de routeur MR que le routeur MR (120) peut extraire de tests MNNT qu'il reçoit pour un routage au noeud MNN (110).

13. Procédé de communication validée selon l'une quelconque des revendications précédentes, dans lequel le processus de validation (200) entre le routeur mobile, MR, (120) et le noeud correspondant, CN, (150) comporte l'étape ci-dessous dans laquelle:

le routeur MR (120) compare sa propre adresse au bon soin (142) à une quelconque adresse CoA que le routeur MR (120) peut extraire de tests MNNT qu'il reçoit pour un routage au noeud MNN (110).

14. Procédé de communication validée selon l'une quelconque des revendications 12 et 13, dans lequel si les adresses correspondent:

le routeur MR (120) n'achemine pas le test MNNT davantage;
il vérifie qu'un témoin d'initiation MNNTI extrait du test MNNT correspond à celui envoyé par le routeur MR (120) dans l'initiation MNNTI; et
lorsqu'une correspondance a été vérifiée, il extrait l'index de valeur à usage unique de noeud MNN et un jeton de noeud MNN du test MNNT.

15. Procédé de communication validée selon l'une quelconque des revendications précédentes, dans lequel le processus de validation (200) entre le routeur mobile (MR) (120) et le noeud correspondant (CN) (150) comporte l'étape ci-dessous (266) dans laquelle:

le routeur MR (120) génère une clé de validation de mise à jour obligatoire étendue (XBU), KBMNN, (324) du jeton de noeud MNN.

16. Procédé de communication validée selon l'une quelconque des revendications précédentes, dans lequel le processus de validation (200) entre le routeur mobile, MR, (120) et le noeud correspondant, CN, (150) comporte l'étape ci-dessous (276) dans laquelle:

le routeur MR (120) génère une signature de mise à jour obligatoire étendue, XBU, (322) en utilisant une clé de validation KBMNN (324).

17. Procédé selon la revendication 16, dans lequel la signature est basée sur un code d'authentification de message utilisant la clé de validation KBMNN (324).

18. Procédé de communication validée selon l'une quelconque des revendications précédentes, dans lequel la mise à jour obligatoire étendue comporte au moins deux options:

i. adresse de noeud MNN (320); et

ii. signature de mise à jour XBU (322).

19. Procédé de communication validée selon la revendication 18, dans lequel la mise à jour obligatoire étendue comporte en outre une option d'index de valeur à usage unique de noeud MNN (321).

20. Procédé de communication validée selon l'une quelconque des revendications précédentes, dans lequel le processus de validation (200) entre le routeur mobile, MR, (120) et le noeud correspondant, CN, (150) comporte l'étape ci-dessous dans laquelle:

le noeud CN (150) valide une signature à base de clé de validation KBMNN (322) extraite d'une mise à jour XBU (300) reçue par le noeud CN (150) en provenance du routeur MR (120).

21. Procédé de communication validée selon l'une quelconque des revendications précédentes, dans lequel le processus de validation (200) entre le routeur mobile, MR, (120) et le noeud correspondant, CN, (150) comporte l'étape ci-dessous dans laquelle:

le noeud CN (150) ajoute deux entrées à son cache de liaison (BC), dérivées d'une mise à jour XBU validée (300);

i. l'adresse HoA de routeur MR (132) est marquée comme atteignable par le bais de l'adresse CoA de routeur MR (142); et
ii. l'adresse MNNA (112) est marquée comme atteignable par le bais de l'adresse HoA de routeur MR (132).

22. Procédé de communication validée selon l'une quelconque des revendications précédentes, dans lequel le processus de validation (200) entre le routeur mobile, MR, (120) et le noeud correspondant, CN, (150) comporte l'étape ci-dessous dans laquelle:

le noeud CN (150) ajoute deux entrées à son cache de liaison (BC), dérivées d'une mise à jour XBU validée (300):

i. l'adresse HoA de routeur MR (132) est marquée comme atteignable par le bais de l'adresse CoA de routeur MR (142); et
ii. l'adresse MNNA (112) est marquée comme atteignable par le bais de l'adresse CoA de routeur MR (142).

23. Procédé de communication validée selon l'une quelconque des revendications 21 et 22, dans lequel si le noeud MNN (110) est le destinataire, le noeud CN (150) analyse de manière récursive son cache BC; et de sorte que le noeud CN (150) acheminera des paquets pour le noeud MNN (110) avec une desti-

nation d'entête IP d'adresse CoA de routeur MR (142), et avec un entête de routage comportant au moins l'adresse MNNA (412).

24. Procédé de communication validée selon l'une quelconque des revendications 21 et 22, dans lequel si le noeud MNN (110) est le destinataire sous au moins deux routeurs mobiles imbriqués, alors le noeud CN (150) analyse de manière récursive son cache BC;
et de sorte que le noeud CN (150) acheminera des paquets pour le noeud MNN (110) avec une destination d'entête IP de l'adresse au bon soin du routeur mobile de niveau supérieur, et avec un entête de routage comportant au moins les adresses au bon soin de routeurs mobiles subséquents et l'adresse MNNA (112).

25. Procédé de communication validée selon l'une quelconque des revendications 2 à 23, dans lequel le routeur mobile, MR, (120) initie uniquement le processus de validation (200) entre le routeur MR (120) et le noeud correspondant, CN, (150) si au moins l'un des ensembles de conditions ci-dessous est rencontré :

i. le noeud MNN (110) souscrit à un service spécifié;
ii. le noeud CN (150) n'a pas ignoré un nombre seuil de mises à jour XBU précédentes (300);
iii. le noeud CN (150) n'a pas ignoré un nombre seuil de processus de validation; et
iv. le noeud MNN (110) satisfait à une règle d'usage.

26. Procédé de communication validée selon l'une quelconque des revendications 3 à 25, dans lequel l'initiation de test d'adresse domestique, HoTI, et l'initiation de test de noeud de réseau mobile, MNNTI, sont associées, l'initiation de test en résultant comportant un témoin d'initiation TI de noeud MNN/domestique, une adresse HoA de routeur MR (132) et une adresse de noeud MNN (112).

27. Procédé de communication validée selon l'une quelconque des revendications 3 à 25, dans lequel l'initiation de test d'adresse au bon soin, CoTI, et l'initiation de test de noeud de réseau mobile, MNNTI, sont associées, l'initiation de test en résultant comportant un témoin d'initiation TI de noeud MNN/au bon soin, une adresse CoA de routeur MR (142) et une adresse de noeud MNN (112).

28. Procédé de communication validée selon l'une quelconque des revendications précédentes, le procédé comportant en outre l'étape ci-dessous dans laquelle:

le routeur mobile, MR, (120), suite à la réception d'un paquet mis sous tunnel en provenance de son agent domestique, HA, (130), envoie une mise à jour XBU (300) à l'adresse source d'un paquet interne pour une adresse de destination du paquet interne.

29. Procédé de communication validée selon la revendication 28, dans lequel un réseau d'un premier routeur mobile, MR1, (420) comporte un second routeur mobile, MR2, (460), le réseau de routeur MR2 (460) comportant un noeud MNN (410), le procédé comportant les étapes ci-dessous dans lesquelles:

suite à la réception d'un premier paquet mis sous tunnel, le routeur MR1 (420) envoie une mise à jour XBU (401) à l'agent domestique du routeur MR2, HA2, (470) pour l'adresse CoA de routeur MR2 (482) ;
le routeur MR1 (420) achemine un paquet interne au routeur MR2 (460);
le routeur MR2 (460), suite à la réception du paquet, envoie une mise à jour XBU (402) au noeud CN (450) pour l'adresse MNNA (412) ;
suite à la réception d'un second paquet mis sous tunnel envoyé directement à l'adresse CoA de routeur MR2 (482) avec un entête de routage comportant l'adresse HoA de routeur MR2 (472) et l'adresse MNNA (412), l'agent HA1 (430) l'intercepte et met sous tunnel un paquet interne à l'adresse CoA de routeur MR1 (442) ; et
le routeur MR1 (420), suite à la réception du paquet, envoie une mise à jour XBU (403) au noeud CN (450) pour l'adresse CoA de routeur MR2 (482) ;
et de sorte que les quatre entrées ainsi générées dans le cache BC de noeud CN, lorsqu'elles sont analysées de manière récursive, achemineront des paquets pour le noeud MNN (410) avec une destination d'entête IP d'adresse CoA de routeur MR1 (442), et avec un entête de routage d'agent HoA de routeur MR1 (432), d'adresse CoA de routeur MR2 (482), d'agent HoA de routeur MR2 (472), et d'adresse MNNA (412).

30. Procédé de communication validée selon l'une quelconque des revendications 1 à 27, le procédé comportant en outre l'étape ci-dessous dans laquelle:

le routeur mobile, MR, (120), suite à la réception d'un paquet mis sous tunnel en provenance de son agent domestique, HA, (130), envoie une mise à jour XBU (300) à une adresse source d'un paquet le plus interne pour une adresse de destination du paquet interne.

31. Procédé de communication validée selon la revendication 30, dans lequel un réseau d'un premier rou-

teur mobile, MR1, (420) comporte un second routeur mobile, MR2 (460), le réseau de routeur MR2 (460) comportant un noeud MNN (410), comportant les étapes ci-dessous dans lesquelles:

suite à la réception d'un premier paquet mis sous tunnel, le routeur MR1 (420) envoie une mise à jour XBU (601) à l'adresse source du paquet le plus interne, CN, pour l'adresse CoA de routeur MR2 (482) ;
le routeur MR1 (520) transmet le paquet interne au routeur MR2 (460) ;
suite à la réception du paquet interne, le routeur MR2 (460) envoie une mise à jour XBU (602) à l'adresse source du paquet le plus interne (CN) pour le noeud MNN;
et de sorte que les quatre entrées ainsi générées dans le cache BC de noeud CN, lorsqu'elles sont analysées de manière récursive, achemineront des paquets pour le noeud MNN (510) avec une destination d'entête IP d'adresse CoA de routeur MR1 (542), et avec un entête de routage d'adresse HoA de routeur MR1 (532), d'adresse CoA de routeur MR2 (582), d'adresse HoA de routeur MR2 (572) et d'adresse MNNA (512).

32. Dispositif destiné à être utilisé dans une communication validée conformément à un procédé selon l'une quelconque des revendications 1 à 31, entre un noeud de réseau mobile, MNN, (110) et un noeud correspondant, CN, (150) via au moins un premier routeur mobile, MR, (120), et comportant:

i. un moyen de vérification pour mettre en oeuvre un processus de validation (200) dans lequel le message d'initiation de test MNN, MNNTI, est envoyé par le routeur MR (120), et un message de test MNN, MNNT, est envoyé par le noeud CN (150); et
ii. un moyen de mise à jour obligatoire étendue pour envoyer (276), à partir du routeur MR (120), une mise à jour obligatoire étendue (XBU) comportant l'adresse de noeud MNN, MNNA, (112).

33. Routeur mobile, MR, (120) destiné à une connexion avec au moins un appareil supplémentaire pouvant être mis en réseau IP, en communication, par un procédé selon l'une quelconque des revendications 1 à 31, le routeur MR (120) comportant un moyen de message d'initiation de test de noeud de réseau mobile, MNN, MNNTI, pour générer et envoyer un message d'initiation MNNTI, et un moyen de mise à jour obligatoire pour générer et envoyer une mise à jour obligatoire étendue, XBU, (300) comportant l'adresse de noeud MNN, MNNA, (112).

34. Noeud correspondant, CN, (150) destiné à une connexion avec au moins un appareil pouvant être mis en réseau IP, en communication, par un procédé selon l'une quelconque des revendications 1 à 31, le noeud CN (120) comportant un moyen de message de test de noeud de réseau mobile, MNN, MNNT, pour générer et envoyer un message de test MNNT, et un moyen de validation pour valider une signature à base de clé de validation de mise à jour obligatoire étendue, KBMNN, (322) extraite d'une mise à jour obligatoire étendue, XBU, (300).

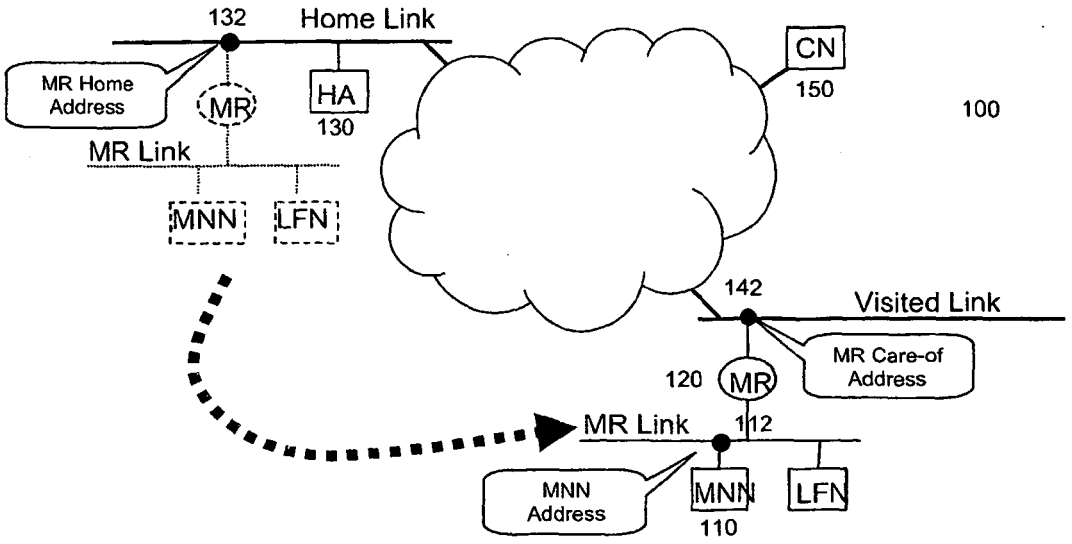
132
Home Link
MR Home Address
MR
HA
130
MR Link
MNN
LFN
CN
150
100
142
Visited Link
MR Care-of Address
120
MR
MR Link
112
MNN Address
MNN
110
LFN

FIG. 1

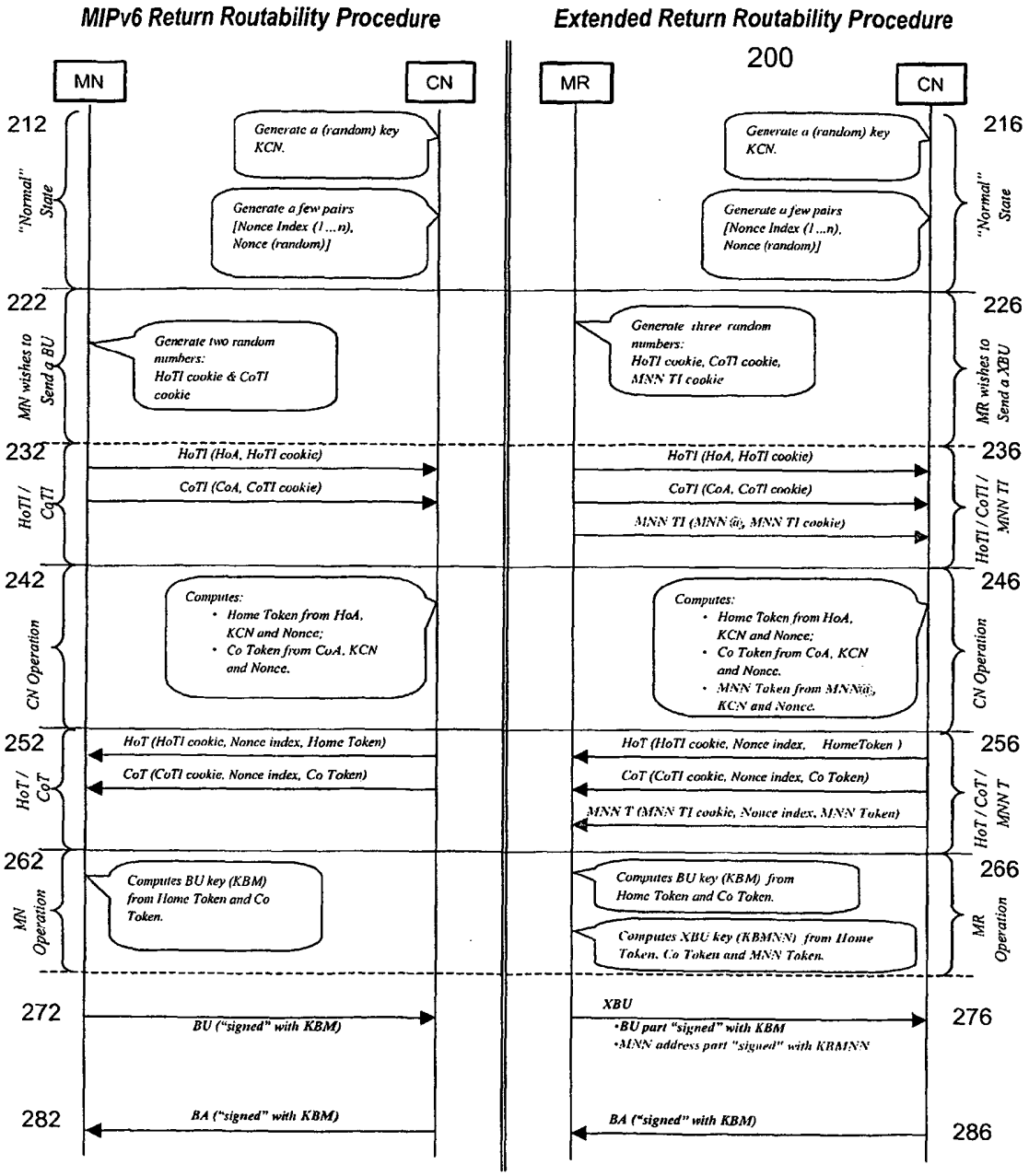
MIPv6 Return Routability Procedure
Extended Return Routability Procedure
200
MN
CN
MR
CN
212
"Normal" State
Generate a (random) key KCN.
Generate a few pairs [Nonce Index (1 ...n), Nonce (random)]
216
"Normal" State
Generate a (random) key KCN.
Generate a few pairs [Nonce Index (1 ...n), Nonce (random)]
222
MN wishes to Send a BU
Generate two random numbers: HoTI cookie & CoTI cookie
226
MR wishes to Send a XBU
Generate three random numbers: HoTI cookie, CoTI cookie, MNN TI cookie
232
HoTI / CoTI
HoTI (HoA, HoTI cookie)
CoTI (CoA, CoTI cookie)
236
HoTI / CoTI / MNN TI
HoTI (HoA, HoTI cookie)
CoTI (CoA, CoTI cookie)
MNN TI (MNN@, MNN TI cookie)
242
CN Operation
Computes:
• Home Token from HoA, KCN and Nonce;
• Co Token from CoA, KCN and Nonce.
246
CN Operation
Computes:
• Home Token from HoA, KCN and Nonce;
• Co Token from CoA, KCN and Nonce.
• MNN Token from MNN@, KCN and Nonce.
252
HoT / CoT
HoT (HoTI cookie, Nonce index, Home Token)
CoT (CoTI cookie, Nonce index, Co Token)
256
HoT / CoT / MNN T
HoT (HoTI cookie, Nonce index, HomeToken)
CoT (CoTI cookie, Nonce index, Co Token)
MNN T (MNN TI cookie, Nonce index, MNN Token)
262
MN Operation
Computes BU key (KBM) from Home Token and Co Token.
266
MR Operation
Computes BU key (KBM) from Home Token and Co Token.
Computes XBU key (KBMNN) from Home Token, Co Token and MNN Token.
272
BU ("signed" with KBM)
XBU
•BU part "signed" with KBM
•MNN address part "signed" with KBMNN
276
282
BA ("signed" with KBM)
BA ("signed" with KBM)
286

FIG. 2

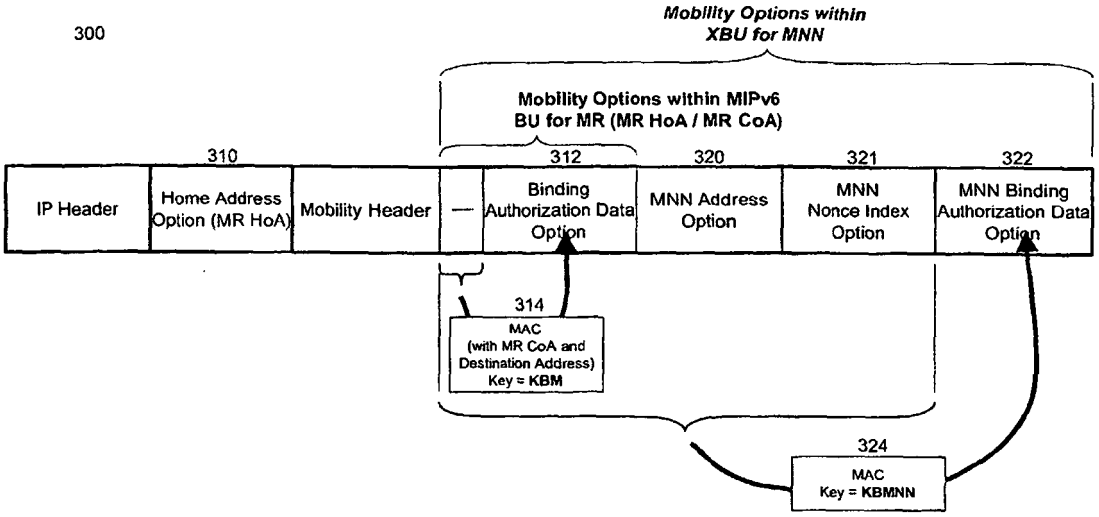
300
Mobility Options within XBU for MNN
Mobility Options within MIPv6 BU for MR (MR HoA / MR CoA)
310
312
320
321
322
IP Header
Home Address Option (MR HoA)
Mobility Header
—
Binding Authorization Data Option
MNN Address Option
MNN Nonce Index Option
MNN Binding Authorization Data Option
314
MAC (with MR CoA and Destination Address) Key = KBM
324
MAC Key = KBMNN

FIG. 3

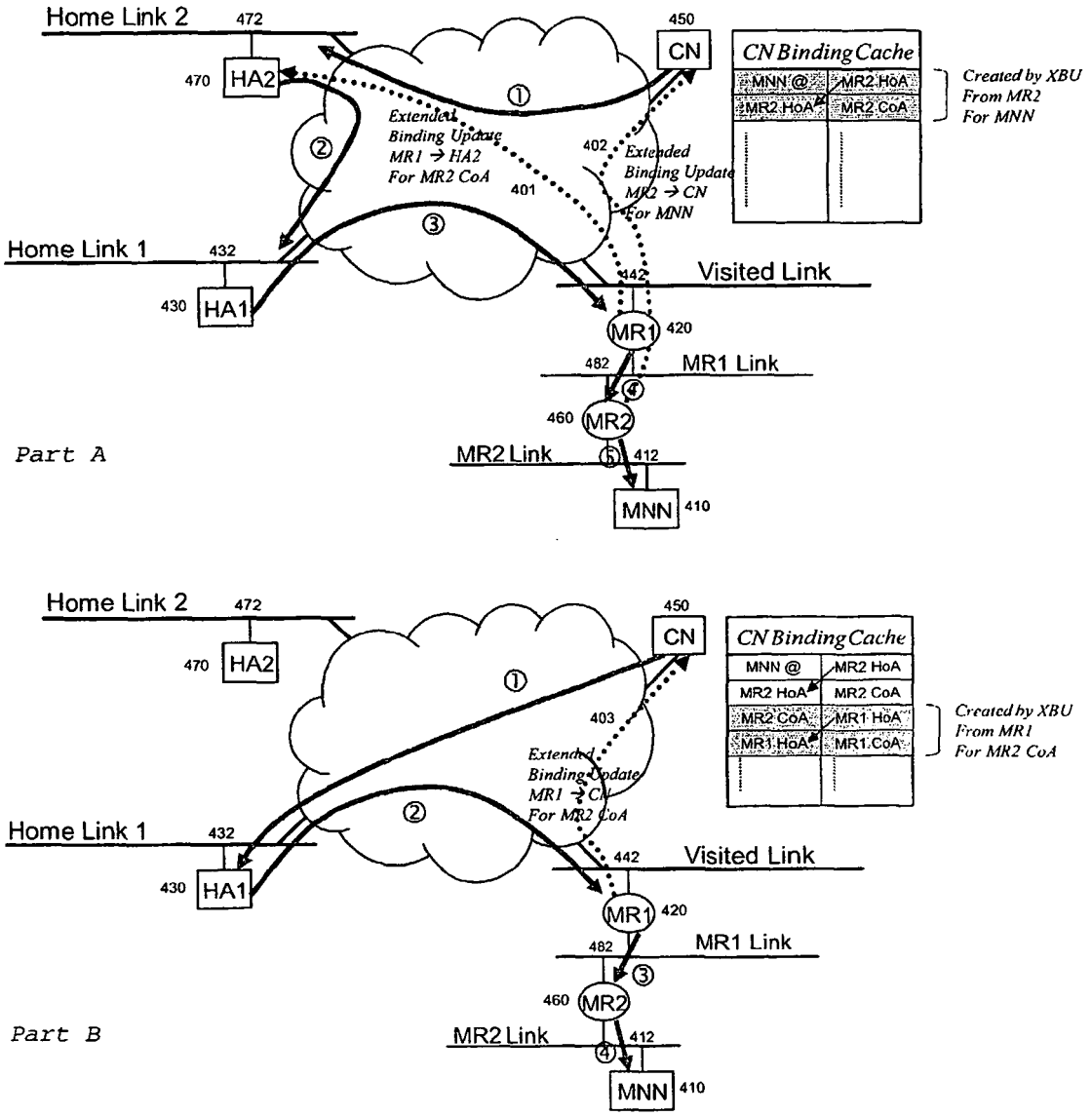
Home Link 2
472
470
HA2
450
CN
CN Binding Cache
MNN @
MR2 HoA
MR2 HoA
MR2 CoA
Created by XBU
From MR2
For MNN
①
②
③
Extended
Binding Update
MR1 → HA2
For MR2 CoA
401
402
Extended
Binding Update
MR2 → CN
For MNN
Home Link 1
432
430
HA1
442
Visited Link
MR1
420
482
MR1 Link
④
460
MR2
MR2 Link
⑤
412
MNN
410
Part A
Home Link 2
472
470
HA2
450
CN
CN Binding Cache
MNN @
MR2 HoA
MR2 HoA
MR2 CoA
MR2 CoA
MR1 HoA
MR1 HoA
MR1 CoA
Created by XBU
From MR1
For MR2 CoA
①
②
403
Extended
Binding Update
MR1 → CN
For MR2 CoA
Home Link 1
432
430
HA1
442
Visited Link
MR1
420
482
MR1 Link
③
460
MR2
MR2 Link
④
412
MNN
410
Part B

FIG. 4

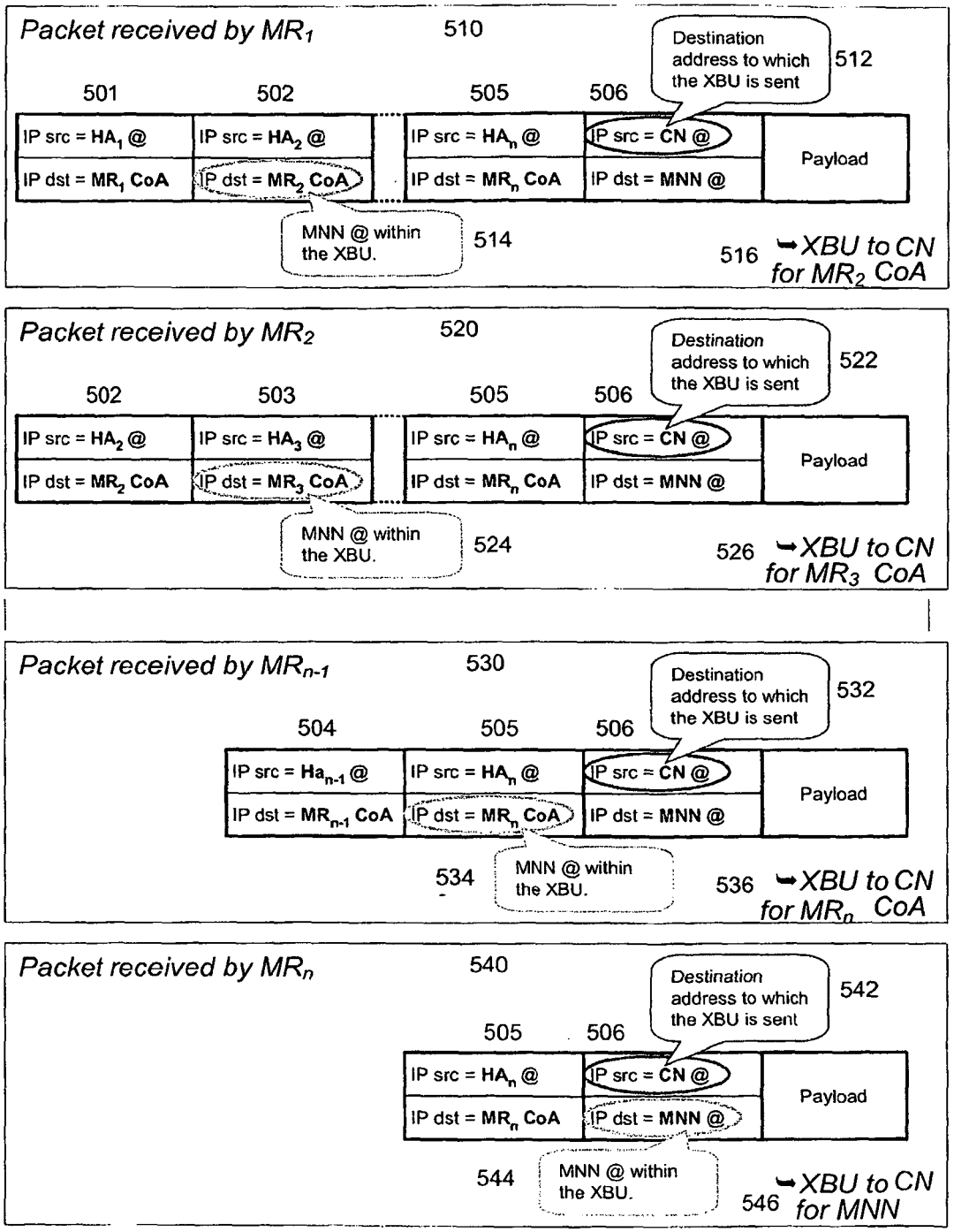
Packet received by MR1
510
Destination address to which the XBU is sent
512
501
502
505
506
IP src = HA1 @
IP dst = MR1 CoA
IP src = HA2 @
IP dst = MR2 CoA
IP src = HAn @
IP dst = MRn CoA
IP src = CN @
IP dst = MNN @
Payload
MNN @ within the XBU.
514
516
XBU to CN for MR2 CoA
Packet received by MR2
520
Destination address to which the XBU is sent
522
502
503
505
506
IP src = HA2 @
IP dst = MR2 CoA
IP src = HA3 @
IP dst = MR3 CoA
IP src = HAn @
IP dst = MRn CoA
IP src = CN @
IP dst = MNN @
Payload
MNN @ within the XBU.
524
526
XBU to CN for MR3 CoA
Packet received by MRn-1
530
Destination address to which the XBU is sent
532
504
505
506
IP src = Han-1 @
IP dst = MRn-1 CoA
IP src = HAn @
IP dst = MRn CoA
IP src = CN @
IP dst = MNN @
Payload
534
MNN @ within the XBU.
536
XBU to CN for MRn CoA
Packet received by MRn
540
Destination address to which the XBU is sent
542
505
506
IP src = HAn @
IP dst = MRn CoA
IP src = CN @
IP dst = MNN @
Payload
544
MNN @ within the XBU.
546
XBU to CN for MNN

FIG. 5

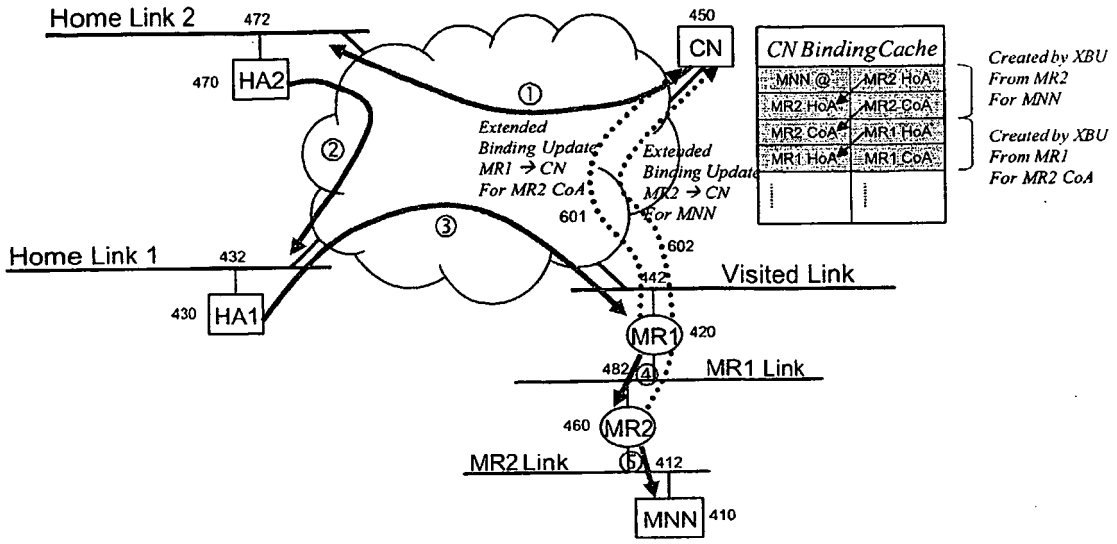
Home Link 2
472
470
HA2
450
CN
CN Binding Cache
MNN @
MR2 HoA
MR2 HoA
MR2 CoA
MR2 CoA
MR1 HoA
MR1 HoA
MR1 CoA
Created by XBU
From MR2
For MNN
Created by XBU
From MR1
For MR2 CoA
①
②
③
④
⑤
Extended
Binding Update
MR1 → CN
For MR2 CoA
601
Extended
Binding Update
MR2 → CN
For MNN
602
Home Link 1
432
430
HA1
442
Visited Link
MR1
420
482
MR1 Link
460
MR2
MR2 Link
412
MNN
410

FIG. 6

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- EP 1158742 A1 **[0010]**
- US 20030095523 A **[0011]**
- EP 02291331 A **[0080]**